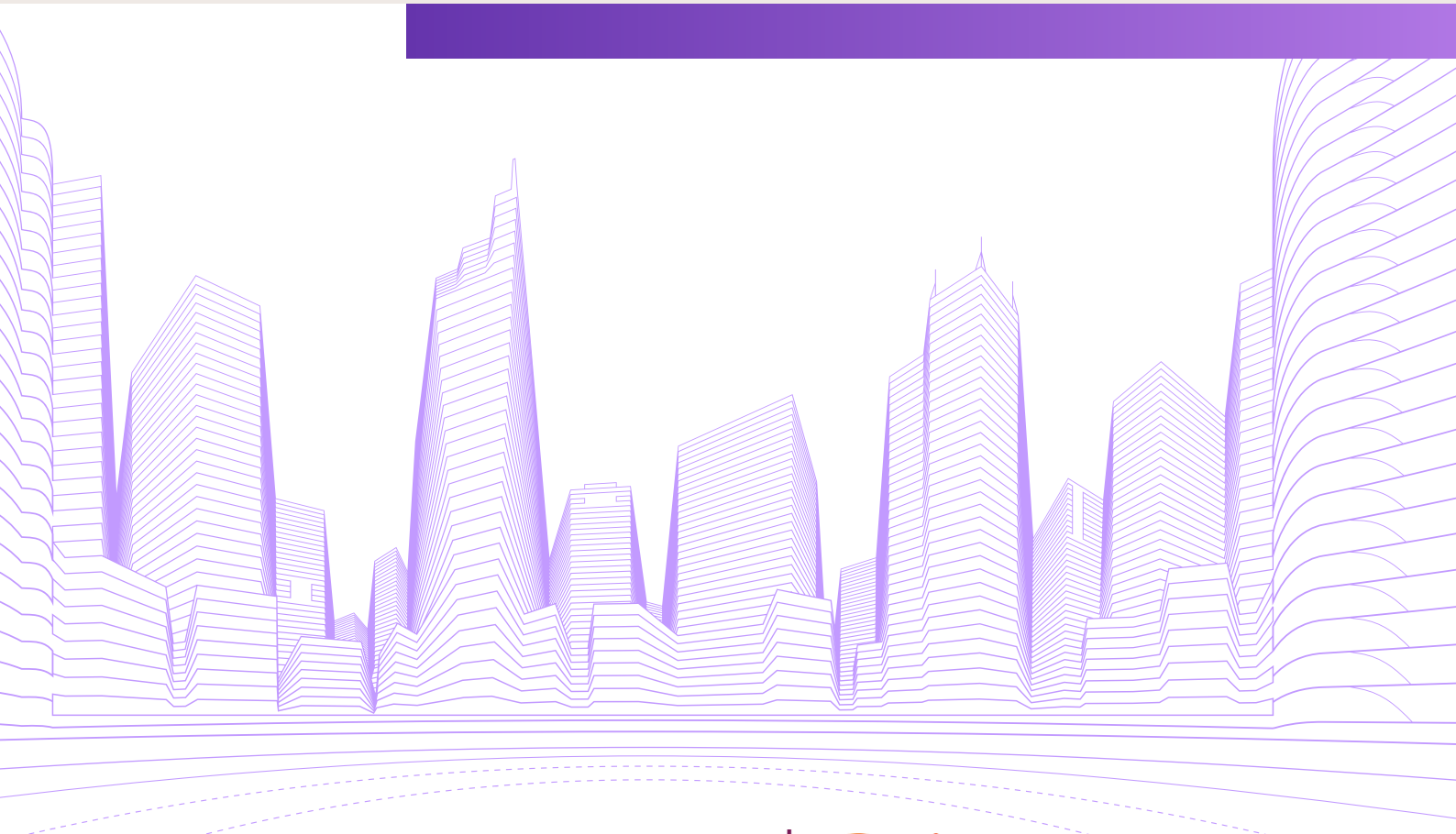
WHITEPAPER

Cloud vs. On-Premises for FSCS SCV Reporting: What Should Financial Institutions Choose?



macro global®
creating value through innovation

SASF

Table of Contents

Introduction

The UK financial services industry is confronted with a sophisticated and constantly changing panorama of regulatory reporting, with FSCS Single Customer View (SCV) requirements being a fundamental cornerstone. The challenge surpasses mere compliance; it requires strong data integrity, operational resilience, and nimble flexibility to constant change. Choosing the suitable deployment model – traditional on-premises infrastructure or dynamic cloud – is no longer merely a technological decision. This strategic decision has far-reaching implications for efficiency, security, and future innovation.

This white paper provides practical advice based on leading-edge industry trends and real-world experience, enabling financial institutions to make a well-informed decision regarding their SCV reporting future.

Current Industry Landscape & Emerging Trends

The financial services sector is undergoing a profound digital transformation, radically altering the way institutions operate and interact with their clientele. This seismic change has a direct, material effect on regulatory reporting, specifically for business-critical obligations such as FSCS Single Customer View (SCV). Regulatory reporting in the past has traditionally been perceived as a back-office activity, an obligatory but detached chore. Today, however, the demand for efficiency, precision, and real-time visibility necessitates a much more integrated and technology-enabled solution.

This technological revolution aligns with an age of increasing regulatory oversight and complexity for FSCS SCV regulation. Regulators require increased transparency, higher granularity, and demonstrably sound processes for data aggregation and reconciliation. The disintegrated data environments so common in much of the old-line financial sector–full of redundancies and silos–is simply no longer viable under this added pressure. Lack of a complete view of customer behaviour and risk profiles across different regulatory segments because of disintegrated data is a particular worry, heightening the risk of mistakes and non-compliance.

To counteract these pressures, a major trend has been the increased uptake of cloud-based Software as a Service (SaaS) solutions in regulated environments. Financial institutions are increasingly seeing the built-in benefits of the cloud, including scalability, cost-effectiveness, and improved security postures provided by trusted cloud vendors, which can exceed individual FI capabilities. Recent industry reports and surveys all consistently point to this trend, as numerous FIs are making significant use of cloud platforms to boost their operational agility and resilience in

managing data and reporting. This trend is prompted by a keen awareness that cloud services can deliver the elastic infrastructure and sophisticated capabilities required for handling varying amounts of data and intricate regulatory calculations effectively.

In addition, hybrid and multi-cloud strategies have become a practical middle ground for most institutions. By using this method, FIs can keep confidential information or back-end systems on premises but make use of the cloud for elastic processing, analytics, and business continuity/disaster recovery. Having a multi-cloud approach with offerings from multiple vendors will also further improve resilience and prevent vendor lock-in. These hybrid solutions facilitate phased migration to the cloud and enable FIs to modernise infrastructure gradually while maintaining risk management and ongoing compliance. This strategic fusion provides the control and comfort of on-premises deployments with the agility and innovation of the cloud, which was instrumental in coping with the changing needs of FSCS SCV reporting.

Understanding the Deployment Options

Feature	On-Premises	Cloud (SaaS)	Hybrid
Control & Ownership	High (FI owns and manages all hardware/software)	Low to Moderate (Vendor owns/ manages, FI controls data and configurations)	Mixed (FI controls some infrastructure, vendor controls cloud components)
Infrastructure	Housed within FI's physical data centres	Hosted by a third-party cloud provider (e.g., AWS, Azure, Google Cloud)	Combination of on-premises and cloud infrastructure
Management	Entirely managed by FI's internal IT team	Largely managed by the SaaS vendor, reducing FI's operational burden	Shared responsibility between FI and cloud provider
Upfront Costs	High (CAPEX for hardware, software licenses, setup)	Low (Subscription-based, OPEX model)	Moderate (Mix of CAPEX and OPEX)
Ongoing Costs	High (Maintenance, power, cooling, upgrades, dedicated staff)	Predictable (Subscription fees, based on usage)	Variable (Combines ongoing costs of both models)
Scalability	Limited; time-consuming and costly to scale up/down	Highly elastic and on-demand; easy to scale up or down as needed	Flexible scaling; can burst to cloud for peak loads
Agility/ Innovation	Slower deployment cycles; limited access to cutting-edge cloud services	Rapid deployment; access to advanced technologies (AI/ML, analytics)	Increased agility for certain workloads; flexibility in technology adoption

Feature	On-Premises	Cloud (SaaS)	Hybrid
Security	FI is solely responsible for entire security stack	Shared responsibility model; cloud provider manages infrastructure security, FI manages data/app security	Complex; requires consistent security policies across environments
Disaster Recovery	Complex and expensive to set up and maintain	Often built-in, highly resilient, and cost-effective	Can leverage cloud for cost-effective DR of on-premises systems

The argument between these models is usually muddied by past perceptions and a misunderstanding of current capabilities. Financial institutions making this decision often face the following misconceptions:

Misconception 1: "On-premises provides better security and control over sensitive data."

Reality: Although on-premises seems more contained, contemporary cloud providers allocate billions to security infrastructure, skills, and certifications (e.g., ISO 27001, SOC 2) that frequently surpass those of individual FIs. FIs' actual challenge, no matter what model, is maintaining a strong security setup and governance. Cloud providers use a "shared responsibility model," whereby the provider secures the cloud itself, and the customer secures in the cloud (their data, apps, configurations).

Misconception 2: "Cloud data residency is a significant compliance roadblock for UK FIs."

Reality: Large cloud vendors now have region-restricted data centres, enabling FIs to store their data within a particular geography (e.g., the UK) to meet data residency requirements. Regulators such as the FCA have also issued comprehensive guidance on outsourcing and taking up the cloud, emphasising stringent due diligence, monitoring, and exit strategies, not a blanket prohibition.

Misconception 3: "Cloud solutions are always cheaper."

Reality: Although cloud removes high initial CAPEX, the "pay-as-you-go" strategy could result in surprise expenses if not dealt with carefully. A genuine total cost of ownership (TCO) analysis for on-premises (maintenance, power, cooling, workforce, refresh cycles) and cloud (data transfer charges, egress fees, surprise spikes in usage) is important. Usually, for scalable and responsive solutions, cloud is cheaper in the long term, but it needs to be monitored closely.

Misconception 4: "Cloud migration is a 'rip and replace' of all current systems."

Reality: The emergence of hybrid cloud approaches and interoperability solutions allows FIs to adopt the cloud incrementally. FIs can leave some legacy systems on-premises while taking advantage of the cloud for new apps, data analytics, or for particular regulatory workloads such as SCV, enabling a phased and less painful modernisation journey. This enables FIs to keep existing investments and transition to the cloud slowly.

Misconception 5: "Regulatory authorities are naturally suspicious of cloud adoption for critical financial information."

Reality: Regulators worldwide, the FCA included, have increasingly recognised the advantages of cloud computing for financial services if FIs have good governance, risk management, and control structures in place. Regulators are concerned with ensuring security, resilience, and data integrity rather than prohibiting specific technologies altogether. The basis is due diligence and monitoring over time on the part of cloud service providers.

Critical Decision-Making Criteria for FSCS SCV Reporting Solutions

To make this important decision between cloud and on-premises solutions, FIs need to carefully analyse some critical factors, learning how each model deals with their specific requirements in a changing regulatory context.

Compliance and Regulatory Mandates: Conforming to Changing Rules

Compliance is the primary driving force behind any SCV solution. But the regulatory environment is constantly changing, with new rules and amendments frequently appearing. The selected deployment model needs to be inherently able to keep up and respond quickly and effectively.

- **On-Premises:** Despite providing perceived direct control of infrastructure, on-premises solutions may lack agility with fast-paced regulatory updates. It is often time-consuming to roll out changes through manual reconfigurations, prolonged testing, and heavy utilisation of IT resources, resulting in prolonged deployment times and high risk of non-compliance during transition phases. The responsibility for ensuring the system stays compliant with each subtle update lies solely in the hands of the FI.

- **Cloud:** Financial services cloud providers are designed for agility. They constantly evolve their platforms to meet new industry standards and regulation needs. This typically translates to FIs enjoying automated upgrades, compliance frameworks already installed, and rapid scaling of resources to handle the new reporting requirements and being "regulator-ready" with the updates being deployed within 24 hours or less. The shared responsibility model enables FIs to take advantage of the provider's know-how about core compliance infrastructure.

Data Sovereignty and Jurisdictional Concerns: What Recent Regulations Say

Data sovereignty – the notion that data is governed according to the laws and rules of the nation where it is gathered and processed – has long been a major impediment to cloud adoption by FIs. But things have evolved quite a bit:

- **On-Premises:** Offers the most direct route to data residency since data is within the direct physical control of the FI and within a particular jurisdiction. This relieves short-term fears regarding cross-border data transfer and foreign legal oversight.
- **Cloud:** Large CSPs now provide region-based data centres, enabling FIs to select where their data would be located, thus mitigating most data sovereignty issues. Regulations such as GDPR have also provided clarification of data transfers' requirements, focusing on proper protection mechanisms rather than mandating the precise physical location. FIs need to perform rigorous due diligence to verify that CSP contracts and security measures comply with exacting jurisdictional requirements and that they enable compliance with individuals' rights in GDPR, such as access, correction, and erasure.

Integration with Existing Legacy Systems and Data Workflows

Financial institutions usually run with a mature ecosystem of legacy systems and well-formed data flows. The SCV solution needs to fit in without major disruption or introducing new data silos:

- **On-Premises:** Integration with existing on-premises legacy systems may appear simpler since it's in the same environment. But here too, there are often intricate custom integrations, point-to-point links, and manual data mapping because of heterogeneous data formats and technologies.

- **Cloud:** Contemporary cloud SCV solutions are built with interoperability in mind. Solutions such as SCV Forza feature hassle-free, pre-configured connectors for all leading Core Banking Systems (CBS), avoiding expensive and time-consuming custom integration. They use APIs and powerful data integration capabilities to handle disparate data formats and enable cleansing, enrichment, and automated reconciliation of data, building a perfect "golden source of truth" from disjointed legacy systems.

Scalability and Agility Requirements in Dynamic Regulatory Environments

The speed and volume of financial information are increasing all the time, and regulatory authorities often impose new reporting obligations that require scalable and agile IT infrastructure:

- **On-Premises:** Scaling an on-premises SCV solution up or down is capital- and time-consuming. It requires buying and installing new hardware, setting up software, and dealing with physical infrastructure. This inbuilt inflexibility critically constrains an FI's ability to respond quickly to unexpected surges in data volumes or pressing new regulatory requirements.

- **Cloud:** Cloud offerings provide unmatched scalability and responsiveness. FIs can dynamically provision or de-provision resources as they are consumed, only paying for actual usage. SCV Forza-type solutions are designed to process large sets of data, handling 50+ million records per batch with ease. This flexibility enables FIs to quickly respond to shifting data loads and new regulatory requirements without a large initial investment or delays, maintaining business continuity even in the event of an outage. This built-in flexibility eliminates the burden of managing infrastructure and enables FIs to concentrate on outcomes from compliance instead of operational specifics.

Security Posture and Best Practices: Strengthening FSCS SCV Data

FSCS SCV reporting, including personal information, account balances, and financial transactions, is an obvious target for cybercriminals, and therefore strong security protocols are not an option. Incidents in this area not only result in heavy monetary fines but also lose customer confidence and brand equity.

For on-premises setups, critical security controls encompass tight physical controls over data centres, careful network segmentation to segregate the important systems, and a tight patch management program to quickly fix vulnerabilities. Data encryption in transit and at rest, together with end-to-end access controls, are also important.

In cloud SaaS implementations, security is shared responsibility, yet the responsibility lies with the FI to have strong controls. Priorities include taking advantage of the encryption abilities of the cloud provider (for data at rest and in transit), the use of multi-factor authentication (MFA) across all access, and ongoing monitoring of cloud infrastructure. FIs should place their top choice among industry-leading compliance certifications such as ISO 27001 and SOC 2, which illustrate compliance with strict security standards.

Analysing a vendor's security posture requires rigorous due diligence, examining their certifications, security design, incident response planning, and service level agreements. Familiarity with the shared responsibility model is imperative: while the cloud provider protects the "cloud", the FI must protect security in the cloud, such as data, applications, and configurations. Actual instances of security violations in real-world financial regulatory environments, including revealed customer information or system weaknesses, are a stark reminder of the absolute necessity of these controls, no matter the deployment scenario.

Long-Term Strategic Advantage of SaaS to FSCS SCV Reporting

Adopting a Software-as-a-Service (SaaS) architecture for FSCS SCV reporting is more than simply infrastructure selection; it represents a deep-seated strategic evolution that reveals powerful long-term advantage for financial institutions. The responsiveness, productivity, and creativity that reside in SaaS products place FIs not only in a position to comply with regulatory requirements, but to succeed within a changing world.

A key benefit is **quicker time-to-market and ongoing compliance enhancements**. With SaaS, the need for manual patching and upgrades is eliminated as the provider regularly updates the platform to align with changing FSCS and FCA regulations. It always keeps FIS regulator-ready, without the cost of internal IT overhead.

In addition to this, **SaaS is highly cost-optimising**. It also changes the financial model from a capital-intensive CapEx load to a manageable OpEx, releasing capital for reallocation to core business expansion. A thorough 5-10-year Total Cost of Ownership (TCO) analysis reliably proves the long-term cost savings versus keeping burdensome on-premises infrastructure.

Better disaster recovery and business continuity are inherent to cloud resilience. SaaS vendors create highly geographically dispersed and redundant architectures, keeping SCV data and reporting functionality available even under extreme outages, greatly de-risking essential compliance functions.

Most importantly, **SaaS encourages greater innovation and futureproofing.** Cloud-based platforms are the natural home for next-generation technologies. This provides FIs with instant access to AI/ML-powered reporting tools able to validate data, detect patterns, and offer greater insights, constantly raising their reporting game. Success stories of early adopters always show tangible results, ranging from shorter reporting cycles to better data accuracy and lower operational expenses.

Challenges and Considerations for SaaS Adoption

To embrace SaaS for FSCS SCV reporting, FIs must strategically navigate inherent challenges.

- **Data migration,** though essential, requires strong planning and aggressive risk mitigation plans to uphold data integrity and avoid interruption throughout the transition.

- **Vendor lock-in concerns** require rigorous due diligence, strong contract negotiation with sufficient exit clauses, and possibly investigating multi-cloud or hybrid approaches to ensure flexibility.

Most importantly, effective SaaS uptake depends on ahead-of-the-game **change management and organizational preparation**. This means building a cloud-first mindset, reskilling internal teams, and communicating advantages to ensure smooth integration and extracting the maximum transformative value of cloud-based SCV solutions.

Hybrid Solutions: Convergence of On-Premises and Cloud for Efficient SCV Reporting

For most financial institutions, a "big bang" move to the cloud is not possible, nor is remaining on-premises entirely ideal. Hybrid models come into picture here as a strong strategic option for FSCS SCV reporting with the best of both worlds: the perceived control and invested leverage of on-premises infrastructure and the agility, scalability, and innovation potential of the cloud.

This strategy enables FIs to keep sensitive core information in their own highly secured environments while using the cloud for dynamic processing, bursting workloads, and advanced analytics.

In real-world use cases for FSCS SCV reporting, hybrid deployment is best for FIs that must:

Gradually Modernise:

- Phase-in parts of their SCV solution in an incremental manner, testing and iterating as they progress.

Balance Data Sensitivity:

- Retain highly sensitive or historical customer data in-house while leveraging cloud capacity for data aggregation, validation, and report generation.

Manage Spikes in Demand:

- Take advantage of cloud elasticity to handle peak reporting seasons without over-provisioning costly on-premises equipment.

Tap Cloud Analytics:

- Leverage cloud-native AI and machine learning capabilities for richer customer behaviour and risk insights, without the need to duplicate whole datasets.

Next-generation technologies are increasingly supporting seamless hybrid management. Unified control planes, containerization (such as Kubernetes), and sophisticated API integrations enable FIs to operate workloads and data on both environments as one unified infrastructure. This strategic combination provides a pragmatic solution to greater security, compliance, and operational efficiency without the need for a jarring overhaul.

Actionable Framework: How to Make the Best Decision for Your Institution

Selecting the best deployment model for FSCS SCV reporting demands a systematic, team-based process, extending beyond technical requirements to include strategic business goals. Financial institutions need to involve the main stakeholders throughout the organisation in order to take a holistic approach and avoid risks.

Checklist of Key Questions to Ask

1

Business Teams:

What are our long-term growth estimates for customer accounts and data volume? How important is agility in responding to new products or market change? Can we use SCV data for greater business intelligence aside from compliance?

2

Compliance Teams:

What are the most demanding data residency and sovereignty standards applicable to our operations? How quickly do regulatory shifts usually happen, and how long does it take currently? What degree of auditability and traceability is not negotiable for regulators?

Actionable Framework: How to Make the Best Decision for Your Institution

3

Security Teams:

What is our existing security posture and risk tolerance for cloud adoption? What are the most significant threats we want to counter, and how do each of the models do so? Are we in possession of the internal technical expertise to operate sophisticated security controls in either platform?

4

IT Teams:

What is the status and life expectancy of our existing infrastructure? What are the estimated 3-5-year CAPEX and OPEX for a strictly on-premises approach? What in-house skill sets exist, and what training or hiring would be required for either approach?

Framework for Risk Evaluation and Vendor Selection

1

Identify Risks:

List specific risks involved in each deployment model (e.g., cloud vendor lock-in, on-prem hardware failure, data breach in either).

2

Mitigation Strategies:

Detail clear mitigation strategies for risks identified under both options.

3

Vendor Due Diligence:

For cloud, thoroughly screen prospective providers on security certifications, SLAs, disaster recovery, and regulatory compliance history. For on-prem software, assess vendor support, update frequency, and integration ability.

Deployment of the Chosen Models

1. Pilot a small, non-mission-critical portion of the SCV reporting process or a subset of data to verify the selected model in a controlled environment.
2. Have precise KPIs for accomplishment in place, such as data processing speed, accuracy levels, operational expenses, adherence to compliance, and system uptime.
3. Have the essential tools for regular monitoring of these KPIs in place.
4. Leverage performance data and stakeholder input to improve the selected solution, adjusting the infrastructure, processes, or vendor arrangements as required.
5. The iterative process permits optimisation and minimises the risk of mass-scale, irretrievable mistakes.

Final Thoughts

As we have explored, both on-premises and cloud options have specific strengths and weaknesses. Yet in an age requiring increased data integrity, fast scalability, and intense security, the cloud increasingly provides the best vehicle for future-proofing compliance.

So, we encourage financial institutions to prioritise long-term strategic dexterity and unshakeable security over short-term cost benefits or perceived control from legacy infrastructure. Investment in effective SCV deployment not only guarantees regulatory compliance but also prepares your organisation to use data to gain a competitive edge and sustainable growth.

Macro Global's SCV Suite is a one-stop solution that simplifies FSCS regulatory reporting for banks and financial institutions. Utilising cloud technology, specifically Microsoft Azure, maximises operational effectiveness by offering transparent data integration, scalability, and robust security mechanisms, and provides instant access to tools and updates, making it the best solution for FSCS SCV reporting in a dynamic regulatory environment.

To discuss how a custom, cloud-native SaaS solution can revolutionise your FSCS SCV reporting, we encourage you to interact with our experts for a consultation or personalised demo.

We are here to help you

macro global®
creating value through innovation

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

Microsoft Gold Partner

amazon web services | Partner Network
TECHNOLOGY PARTNER

ISO 9001:2015 Quality Management System Cert. #: 0922900102

ISO 27001:2013 Information Security Management Cert. #: 09222700102

ISO 27701:2019 Privacy Information Management Cert. #: 09222770102

ISO 27018:2019 PII Protection in Public Clouds Cert. #: 09222701802

Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.